IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH INSTAGRAM ACCOUNT "*quez_otp*" THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	Case No. 3:24-mj-105-WCM

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Neil Mahoney, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), an electronic communications service and/or remote computing service provider headquartered at 1 Meta Way, Menlo Park, California 94025. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Since August 2017, I have been employed as a U.S. Postal Inspector ("Inspector") with the U.S. Postal Inspection Service ("USPIS"). Previously, I was a federal law enforcement officer with the Federal Air Marshal Service from May 2010 to August 2017. As an Inspector, I

investigate offenses that adversely affect the United States mails and have experience investigating financial and violent crimes. I am a graduate of the Federal Law Enforcement Training Center and the USPIS academy.

3. I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I have also been the affiant on search warrants to include search warrants for wireless telephones and social media applications such as Instagram. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that offenses to include 18 U.S.C. § 1704 (*theft of USPS keys*), 18 U.S.C. § 201 (*bribery of public officials*), and 18 U.S.C. § 1349 (*conspiracy to commit financial institution fraud*) have been committed by the user of the Instagram account "*quez_otp*". There is also probable cause to search the items described in Attachment A for evidence and/or instrumentalities of these crimes as described in Attachment B.

4. The facts and information contained in this affidavit are based on my personal knowledge as well as that of other law enforcement involved in this investigation to include the U.S. Postal Service Office of Inspector General ("USPS-OIG") and the Charlotte Mecklenburg Police Department ("CMPD"). This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. §

2711(3)(A)(i).

PROBABLE CAUSE

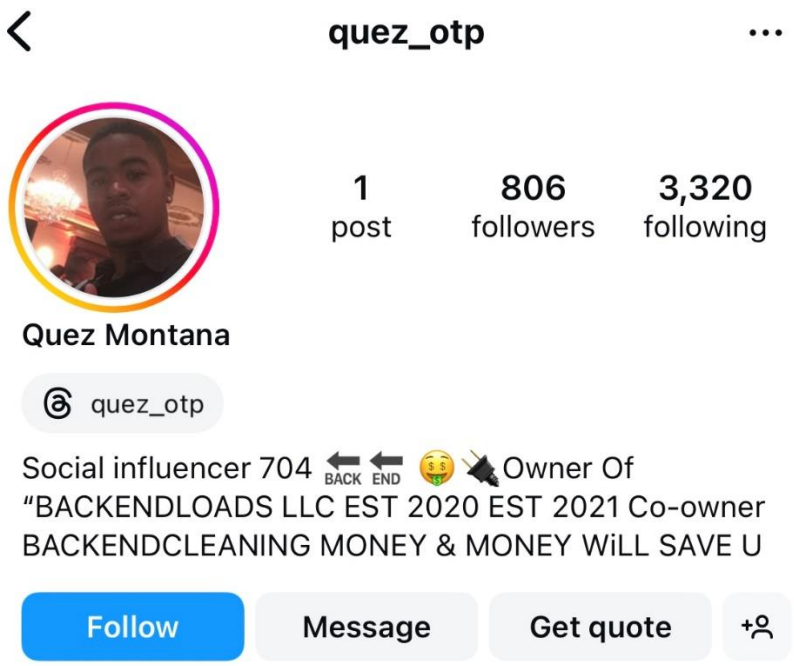
6. In December 2023, I became aware of a subject driving a black Mercedes-Benz ("Mercedes") unlawfully accessing a business park's mail Cluster Box Units ("mailbox") located at 8050 Corporate Center Drive, Charlotte NC 28226 ("Corporate Center") by using a USPS arrow key.[1]

7. On Saturday, January 13, 2024, at approximately 11:50 PM, the subject, later identified as M.H., was observed accessing the Corporate Center mailboxes in the Mercedes and attempting to steal mail. Your affiant and CMPD responded to Corporate Center. CMPD officers attempted to stop the Mercedes by activating their emergency blue lights; however, M.H. fled in the vehicle. CMPD subsequently located M.H. and took them into custody on state charges to include eluding and breaking and entering. CMPD processed M.H.'s vehicle and recovered items to include an Apple iPhone cellular phone, stolen mail from several locations around Charlotte, blank check stock, an electronic label maker, and electronic payment cards not in M.H.'s name. A second cellular phone was recovered from M.H.'s person, and a USPS arrow key, serial number *95-59213*, was recovered from the Corporate Center mailbox.

8. On the afternoon of Sunday, January 14, 2024, M.H. voluntarily agreed to speak with me and other law enforcement officers in an audio and video recorded interview at CMPD. I asked M.H. what happened at Corporate Center the prior evening. M.H. first said they had been smoking in their car and waiting on a friend. After seeing a helicopter and approaching CMPD

[1] Arrow keys are serialized accountable government property that provide authorized USPS employees access to mailboxes. Each arrow key has a unique series and serial number. Arrow keys are valuable to mail thieves as they allow efficient access to potentially large volumes of mail in a single location thereby limiting their risk of detection. Criminals frequently acquire arrow keys from robbing USPS employees or by purchasing them from collusive USPS employees.

vehicles, M.H. said they became scared and fled. After I advised M.H. they had been captured multiple times on surveillance stealing or attempting to steal mail, M.H. admitted they were occasionally stealing for approximately six months when they needed money to support their self and their family. M.H. said other co-conspirators would provide them an arrow key and send text messages with the addresses of business parks where they should steal. M.H. said the locations were frequently in the area around Pineville adjacent to I-485 and they would use their GPS to route themselves to the addresses. After stealing, M.H. said they would turn most of the stolen mail containing checks to co-conspirators and keep some for themself which they would sell through word of mouth or through the social media application Instagram. During the interview, M.H. also stated they communicated regularly with collusive USPS employees and specifically described two that sell stolen mail and USPS keys. M.H. said they communicated with the USPS employees through their cellular phones, and they could purchase a USPS arrow key within one hour. M.H. showed law enforcement their Instagram account on their cellular telephone and the Instagram accounts of the previously mentioned collusive USPS employees. One of the Instagram accounts M.H. identified has the profile name "Quez Montana" and username "*quez_otp*". A profile picture for the account (depicted below) shows a male law enforcement believes to be USPS employee Marquez GASTON, carrier technician, based at Minuet Carrier Annex ("MCA") in Charlotte, NC:



9. On January 16, 2024, a USPIS Physical Security Specialist ("PSS") confirmed arrow key *95-59213*, previously possessed by M.H. and recovered from the Corporate Center mailbox on January 13, 2024, was last assigned to the MCA in December 2023.

10. On January 26, 2024, USPIS executed a federal search warrant for M.H.'s cellular phones seized by law enforcement in January 2024. As a result, a forensic examination was obtained from the devices and data revealed:

11. On June 7, 2023, M.H.'s cellular phone received an Instagram message from the account named "Quez Montana." In the message, Quez Montana utilized emojis consisting of a mailbox and a key which appeared to inform M.H. they had a USPS arrow key available to purchase. A message was sent back from M.H.'s cellular phone asking for the price and Quez Montana responded, "2k."

12. On December 2, 2023, M.H.'s cellular phone reinitiated Instagram messaging with Quez Montana. Specifically, a message was sent from M.H.'s phone asking Quez Montana if they,

"…still got that key?" Quez Montana informed M.H. they did have a key and M.H. told Quez Montana that he had "…cash ready." Another message was sent from M.H.'s phone asking Quez Montana when they were available to meet. Quez Montana responded by saying, "7048408483 call me." Additionally, Quez Montana informed M.H. they could meet them around the time they got off from work, which would be, "…around 7."

13. Thereafter, on December 2, 2023, M.H.'s cellular phone engaged in several phone calls and text messages with telephone number (704) 840-8343 as detailed below:

i. At approximately 7:26 p.m., M.H.'s phone received two phone calls from (704) 840-8343.

ii. At approximately 7:31 p.m., M.H.'s phone placed a call to telephone number (704) 840-8343.

iii. At approximately 7:46 p.m., M.H.'s cellular phone received a text message from telephone number (704) 840-8483 that stated, "I'm here."

iv. At approximately 7:51 p.m., M.H.'s cellular phone sent a text message to (704) 840-8483 that stated, "Pulling here".

v. At approximately 7:53 p.m., M.H.'s phone placed a final phone call to telephone number (704) 840-8343.

14. Later that night on December 2, 2023, at approximately 9:04 p.m., M.H.'s cellular phone texted an image of what appeared to be a USPS arrow key to a contact in their phone listed as "Skooby Doo" with telephone number (704) 430-2084. Skooby Doo sent a text message back to M.H.'s phone that stated, "We a have 2 keys cuh & ya need tell 1 these hoes u want ya hands right." In response, M.H.'s cellular phone sent a message back that stated in part, "I'm tryna get rich…".

15. Agents reviewed records from Verizon, including subscriber information, for telephone number (704) 840-8483. According to those records, telephone number (704) 840-8483 belonged to GASTON since April 2023. Additionally, a review of USPS employee records revealed GASTON has been a carrier technician at the Minuet MCA in Charlotte, NC since approximately June 2022. Moreover, GASTON has been a USPS employee since approximately April 10, 2021. Additionally, USPS time and attendance records for GASTON revealed on December 2, 2023, GASTON was present at work from approximately 8:28 a.m., to 7:24 p.m.

16. On February 6, 2024, a USPIS PSS told me they had been contacted earlier that day by USPS MCA management with the results of a USPS arrow key audit. The MCA manager's audit revealed approximately 17 arrow keys were unaccounted for and missing.

17. On February 26, 2024, I received records from Meta.[2] The Instagram account with the display name "Quez Montana" has records dating back to approximately November 2021. The email associated with the account is quezgaston5@gmail.com and the verified phone number for the account is (704) 840-8483.

18. On February 29, 2024, agents reviewed Instagram Stories posted to the Quez Montana account.[3] The first Instagram story showed a male recognized as GASTON smoking and operating a vehicle. Additionally, the story had a visible caption that read "You ain't got no Motion

[2] According to www.wikipedia.org, Meta Platforms, Inc., doing business as Meta, and formerly named Facebook, Inc., and TheFacebook, Inc., is an American multinational technology conglomerate based in Menlo Park, California. The company owns and operates Facebook, Instagram, Threads, and WhatsApp, among other products and services.

[3] According to www.help.instagram.com, Stories are an Instagram feature where users can share photos and videos that disappear from their profile, Feed and messages after 24 hours, unless they add them to their profile as story highlights. Additionally, sharing a photo or video to an Instagram story is not available via a computer; however, it is available via applications such as the Android app and the iPhone app.

can't get next to Me!!".[4] An additional Instagram story showed a green substance that appeared similar to marijuana inside of a plastic bag labeled "Sharklato."[5]

19. Based on my training and experience, as well as my conversations with other law enforcement officers, stolen mail and USPS arrow keys are frequently sold and marketed on Instagram and Telegram.[6] Moreover, I have seized numerous electronic devices, including cellular phones, related to mail theft investigations that had Instagram and Telegram applications downloaded to the device. The owners of the devices commonly utilized the social media applications for criminal purposes.

[4] According to www.fraudsterglossary.com, motion is slang for making money, having success with fraud, etc.

[5] According to www.leafly.com, Sharklato is a hybrid weed strain made from a genetic cross between Zkittlez and Gelato. Sharklato is 20% THC, making this strain an ideal choice for both beginners and experienced cannabis consumers.

[6] According to www.telegram.org, Telegram Messenger is a globally accessible encrypted cloud-based centralized instant messaging service. The application provides optional end-to-end encrypted chats, file sharing and other features. Cloud chats and groups chats are encrypted between the client and the server, so that ISPs (internet service provider) and other third parties on the network can't access data. Users can send text/voice messages, make voice/video calls, and share an unlimited number of images, documents, user locations, animated stickers, contacts, and audio files. Users can also follow channels. Telegram accounts are usually tied to telephone numbers which are verified by SMS (short message service) or phone call. Account creation requires an iOS or Android device regardless of the platform intended to be used. Users can add multiple devices to their account and receive messages on all of them. Telegram's default messages are cloud-based. Users can send messages to other users individually or in groups of up to 200,000 members. Sent messages can be edited up to 48 hours after they have been sent and can be deleted at any time on both sides. Messages can be sent with client-to-client encryption in secret chats. Unlike Telegram's cloud-based messages, messages sent within a secret chat can be accessed only on the device upon which the secret chat was initiated and the device upon which the secret chat was accepted. Messages sent within secret chats can, in principle, be deleted at any time and can optionally self-destruct. In September 2015, Telegram added channels. Channels are a form of one-way messaging where admins can post messages, but other users are not. Any user can create and subscribe to channels. Channels can be created for broadcasting messages to an unlimited number of subscribers. Channels can be publicly available with an alias and a permanent URL so anyone can join. Users who join a channel can see the entire message history. Users can join and leave channels at any time. Depending on a channel's settings, messages may be signed with the channel's name or with the username of the admin who posted them. Non-admin users are unable to see other users who've subscribed to the channel.

20. On March 14, 2024, agents researched telephone number (704) 840-8483 via the Telegram application. Telephone number (704) 840-8483 shows it associated with an active Telegram account as recent as March 12, 2024.

21. Instagram appears to be what GASTON utilized to facilitate the sale of a USPS arrow key to M.H in December 2023. In 2024, an undercover law enforcement officer ("UC") initiated communication with GASTON through the "Quez Montana" Instagram account. On March 19, 2024, the UC met in-person and purchased arrow key *95-58221* from GASTON. On March 20, 2024, a USPIS PSS told me the key was assigned to the MCA as of March 2024. As noted above, arrow keys *95-58221* and *95-59213* (previously possessed by M.H.) were both assigned to GASTON's home station, the MCA.

22. I understand that depending on the user's Instagram and wireless device settings, some Instagram content may remain solely within Meta/Instagram servers and may not be stored locally on the user's physical devices.

23. Based on my training and experience, I know that individuals engaged in financial institution fraud, theft of USPS keys, and bribery schemes, such as the one described above, utilize the messaging function of social media applications like Instagram to communicate about the scheme. These communications can include messages, pictures, and videos. More importantly, these communications can be stored for extended periods of time by Instagram owner Meta. In this case, it is reasonable to believe the "*quez_otp*" Instagram account and profile is associated with GASTON and it has been used to conduct the sale of stolen USPS arrow keys.

BACKGROUND CONCERNING INSTAGRAM[7]

24. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

25. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

26. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

27. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the

[7] The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Data Policy," https://help.instagram.com/519522125107875; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

28. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

29. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

30. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

31. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

32. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

33. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

34. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

35. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed

from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

36. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

37. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

38. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

39. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

40. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

41. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

42. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

43. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

44. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

45. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

46. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, the use of Instagram instant messaging can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

48. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

SUMMARY

49. The investigation has shown that cellular phone(s) and applications installed on those device(s) that are directly associated with GASTON have been utilized to facilitate the sale of a stolen USPS arrow key. Additionally, GASTON is utilizing cellular phone applications such as Instagram to advertise his involvement in what appears to be income from illegitimate sources. Additionally, the telephone number associated with GASTON is tied to his Instagram account and an active Telegram account, which based on my experience is one of the most common ways persons engaged in mail theft and related schemes sell stolen items such as checks and USPS arrow keys. Lastly, the MCA where GASTON is employed has approximately 17 missing USPS arrow keys. For these reasons, the search of GASTON's Instagram account would likely yield evidence and instrumentalities of the alleged offenses.

CONCLUSION

50. Based on the forgoing, I request that the Court issue the proposed search warrant.

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

52. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

s/Neil Mahoney
Neil Mahoney
Postal Inspector
U.S. Postal Inspection Service

This Affidavit was reviewed by SAUSA Eric Frick.

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 21st day of March, 2024, at 1:41 PM

Signed: March 21, 2024

W. Carleton Metcalf
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Instagram account "*quez_otp*" active on, but not limited to, November 1, 2021, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, CA 94025

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 26, 2024, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device

identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers from November 1, 2021, to the present;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, November 1, 2021, to March 21, 2024;

C. All content, records, and other information relating to communications sent from or received by the Account from November 1, 2021, to March 21, 2024, including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing

messages sent from or received by the Account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from November 1, 2021, to March 21, 2024, including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account from November 1, 2021, to March 21, 2024; and

F. All location information, including location history, login activity, information geotags, and related metadata from November 1, 2021, to March 21, 2024.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1704 (theft of USPS keys), 18 U.S.C. § 201 (bribery of public officials), and 18 U.S.C. § 1349 (conspiracy to commit financial institution fraud), those violations involving Marquez Gaston and occurring after November 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. Evidence such as messages, emails, notes, images, videos and/or calls amongst or between co-conspirators in coordination or furtherance of the financial institution fraud, theft of USPS keys, and bribery of public officials scheme;

B. Evidence such as images, messages, documents, and videos detailing potential victim PII (personally identifiable information);

C. Evidence of all financial accounts and bank records, including account information, bank accounts, brokerage accounts, cryptocurrency accounts, merchant accounts, credit cards, debit cards, checkbooks, checks, bills, cancelled checks, wire receipts, automated teller machine receipts, lines of credit and other financial records;

D. Evidence of the identity and location of co-conspirators and victims;

E. Evidence of the disposition of the proceeds of the alleged law violations, including U.S. currency, foreign currency, cryptocurrency (e.g., Bitcoin, Monero, Litecoin), jewelry, precious metals, pre-paid debit cards, financial instruments, and financial

accounts constituting or traceable to the proceeds of the aforementioned law violations, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recovery mnemonics needed by law enforcement to access such items;

F. Evidence concerning the location of other evidence, including electronic devices, financial accounts, email accounts, social media accounts, or other online accounts used in furtherance of the aforementioned law violations;

G. Evidence of user attribution showing who used or owned the "*quez_otp*" account at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

H. Any evidence that constitutes the commission of a criminal offense or contraband, the fruits of crime, or things otherwise criminally possessed; or property designed or intended for use or which has been used as the means of committing a criminal offense, including but not limited to evidence of theft of USPS keys, bribery of public officials, and financial institution fraud conspiracy;

I. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

J. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

K. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and

L. The identity of the person(s) who communicated with the user ID, "*quez_otp*" relating to financial institution fraud, theft of USPS keys, and bribery of public officials scheme including records that help reveal their whereabouts.